PALGO JOURNAL OF AGRICULTURE (PJA)

http://www.palgojournals.org/PJA/Index.htm

REVIEWERS GUIDE

PART A: ***Editorial Office Only***

Manuscript Title: A Lightweight Python-Based Real-Time Intrusion Detection Framework for Flow-Level Network Traffic

Authors: Atanda Maruf Oladele, Engr Abdulkabeer Ghazaly-Agboola

---

OVERALL ASSESSMENT

This manuscript presents a practical implementation of an intrusion detection system using the Isolation Forest algorithm with a user-friendly GUI. The work demonstrates technical competence and addresses a relevant problem in cybersecurity. However, there are several areas where the manuscript could be strengthened to meet publication standards for high-quality academic journals.

DETAILED EVALUATION

1. GENERAL COMMENTS

The manuscript tackles an important problem in network security by proposing a lightweight, accessible solution for intrusion detection. The choice of flow-level analysis and the Isolation Forest algorithm is well-motivated and appropriate for real-time scenarios. The inclusion of a GUI component adds practical value for end users.

Strengths:

- Clear problem identification and motivation
- Practical implementation with user-friendly interface
- Appropriate choice of algorithm for unsupervised anomaly detection
- Good balance between technical detail and accessibility

Areas for Improvement:

- The novelty of the contribution needs clearer articulation what specifically distinguishes this framework from existing implementations?
- The experimental validation could be more comprehensive with multiple datasets and comparative analysis
- Some sections lack sufficient depth and technical detail
- The paper would benefit from discussing computational complexity and scalability limits more explicitly

---

2. ABSTRACT

The abstract effectively summarizes the main contribution and provides context for the work. It touches on all essential elements: problem, approach, methodology, and results.

Strengths:

- Concise and well-structured
- Clearly states the problem and proposed solution
- Mentions key performance indicators

Suggestions for Enhancement:

- Consider adding specific quantitative results (e.g., "achieving 95% detection accuracy with less than 3% false positive rate") earlier in the abstract to immediately demonstrate effectiveness
- The phrase "extensive experiments" is somewhat generic consider being more specific about the experimental setup
- Brief mention of the specific datasets used would strengthen credibility

Grammatical Corrections:

- "The framework leverages the Isolation Forest algorithm integrated with a graphical user interface" → "The framework leverages the Isolation Forest algorithm **and integrates it** with a graphical user interface" (for better flow and clarity)

---

3. INTRODUCTION

The introduction provides adequate context and motivation for the research. It establishes the problem space clearly and positions machine learning as a viable solution.

Strengths:

- Good motivation for the research problem
- Clear progression from problem statement to proposed solution
- Appropriate contextualization of ML in network security

Areas for Enhancement:

- The introduction would benefit from specific statistics or recent incidents that illustrate the growing threat landscape (e.g., growth rates in cyber attacks, costs of breaches)
- Research questions or specific objectives should be explicitly stated
- The unique contributions of this work compared to existing solutions need clearer articulation
- Consider adding a paragraph that outlines the structure of the remaining paper

Grammatical Corrections:

- "has amplified the frequency and complexity" → The grammar is correct, but consider "**have** amplified" if referring to "growth in network connectivity and digital services" as multiple factors
- "enabling systems to **be adaptive** and identify" → "enabling systems to **adapt** and identify" (more concise)

- "provides a scalable balance" → "**provides a** scalable balance" or "**strikes a** scalable balance" (the current phrasing is acceptable but could be more idiomatic)

---

4. RELATED WORK (Section 2)

While this section provides a reasonable overview of relevant approaches, it lacks depth and comprehensive coverage of recent literature.

Strengths:

- Good categorization of ML approaches (supervised, semi-supervised, unsupervised)
- Clear justification for choosing Isolation Forest
- Appropriate discussion of flow-level vs. packet-level data

Significant Areas for Improvement:

- The literature review is quite brief for a research paper,it should be expanded substantially
- More recent work (2023-2024) should be included and discussed in detail
- Specific prior implementations of Isolation Forest for IDS should be reviewed and compared
- Missing discussion of other unsupervised methods (autoencoders, clustering techniques)
- No critical analysis of the limitations of previous approaches
- The transition from general ML methods to your specific contribution could be smoother
- Consider organizing the review thematically (e.g., "Feature Extraction Methods," "Unsupervised Learning Approaches," "Real-time IDS Implementations")

Grammatical Corrections:

- "Random Forests**[,]{.insertion...}** rely on labeled data" → Remove the tracked change markup; simply use "Random Forests**,** rely on labeled data" or better yet: "Random Forests rely on labeled data"
- "face scalability issues" → "**face scalability challenges**" (more formal)

---

5. METHODOLOGY (Section 3)

The methodology section outlines the system architecture but lacks the technical depth expected in a research paper.

Strengths:

- Clear modular structure
- Appropriate choice of technologies
- Figure 1 provides useful visual overview

Critical Areas Requiring Expansion:

5.1 Data Processing Pipeline:

- How is flow level data preprocessed? (normalization, scaling, feature selection)
- What features are extracted from the flow data? (this is crucial!)
- How are missing values or outliers handled?

- What is the data windowing strategy for real-time processing?

5.2 Isolation Forest Implementation:

- Why Isolation Forest specifically over other anomaly detection algorithms? (expand beyond the brief mention)
- What are the hyperparameters and how were they selected?
- How is the contamination parameter determined or adapted?
- What is the training/detection pipeline?

5.3 System Architecture:

- More details on the data flow between modules
- How does the system handle streaming data?
- What is the processing latency?
- Memory and computational requirements?

5.4 GUI Design:

- While mentioned, the GUI's specific features for parameter tuning should be described
- How does the visualization aid decision-making?

Grammatical Corrections:

- "Show Image..." → The image embedding appears in the text flow; ensure it's properly referenced as "Figure 1" in the text before or after, not inline
- "Graphical User Interface (GUI): Built with tkinter, it provides" → "Graphical User Interface (GUI): Built with tkinter, **the GUI** provides" (clearer subject)

---

6. IMPLEMENTATION (Section 4)

This section provides good coverage of the implementation technologies but could be more technically detailed.

Strengths:

- Clear explanation of technology choices
- Good justification for Python ecosystem
- Mentions all major libraries used

Suggestions for Enhancement:

- Provide specific version numbers for key libraries (scikit-learn, tkinter, etc.)
- Include discussion of system requirements (OS, hardware specifications)
- Describe the software architecture pattern used (e.g., MVC, modular design)
- Add a code snippet or algorithm pseudocode for the core detection logic
- Discuss any optimization techniques employed for real-time performance
- Mention how the export functionality works (formats supported, structure of exported data)

Grammatical Corrections:

- "superb support" → "**excellent support**" (more formal for academic writing)

- "which provides optimal implementations of algorithms and model training, evaluation, and performance optimization tools" → This sentence is grammatically correct but quite long; consider: "which provides **efficient** implementations of algorithms **and comprehensive tools** for model training, evaluation, and performance optimization"
- "Besides this, an export facility" → "**Additionally, an export facility**" (more formal)
- "and thereby facilitate" → "**thereby facilitating**" (parallel structure)

---

7. EVALUATION (Section 5)

The evaluation section presents results but lacks comprehensiveness and critical analysis expected in research papers.

Strengths:

- Appropriate use of standard metrics (precision, recall, F1-score)
- Visual representations (confusion matrix, bar chart)
- Multiple evaluation perspectives (classification metrics, model summary)

Critical Areas for Improvement:

7.1 Experimental Setup:

- **Dataset Description:** Which specific benchmark datasets were used? (names, sizes, characteristics)
- **Data Split:** What was the train/test split ratio?
- **Cross-validation:** Was cross validation performed?
- **Baseline Comparisons:** No comparison with other algorithms (SVM, Random Forest, autoencoders) this is a significant omission

7.2 Results Analysis:

- The discrepancy between Table 1 and Table 2 metrics needs explanation (e.g., Accuracy 89% vs. 89.2%, different FPR values)
- The claim "over 95% detection accuracy" in the text contradicts the 89-89.2% in the tables which is correct?
- The recall for anomalies (46%) is quite low this should be discussed as a limitation
- No statistical significance testing
- Missing ROC curves and AUC scores (mentioned as key metrics but not shown)
- No ablation study to understand component contributions

7.3 Performance Metrics:

- Processing time/latency for real-time detection not reported
- Memory consumption not discussed
- Scalability tests with varying data volumes missing

7.4 Contamination Levels:

- "tested under various contamination levels" but only one set of results is shown
- How was the optimal contamination level determined?

Grammatical Corrections:

- "The confusion matrix bar chart generated by the system:****" → Remove the backslash before the line break
- Figure references should be consistently formatted
- "Results indicate the system achieves over 95% detection accuracy" → This needs to be reconciled with the 89% shown in tables, or clarified that this refers to "normal" class only

---

8. DISCUSSION (Section 6)

The discussion provides some insights but lacks depth and critical analysis.

Strengths:

- Acknowledges the privacy advantage of flow level analysis
- Mentions potential limitations
- Notes the extensibility of the system

Areas Requiring Substantial Expansion:

8.1 Limitations Analysis:

- The 46% recall for anomalies is a significant limitation that isn't adequately discussed
- Under what conditions does the system perform poorly?
- What types of attacks might it miss?
- Computational limitations for very large networks?

8.2 Comparative Analysis:

- How does this framework compare to commercial or open-source IDS solutions?
- What are the trade-offs between your approach and alternatives?

8.3 Practical Implications:

- Deployment scenarios and requirements
- Integration challenges with existing security infrastructure
- Training requirements for users

8.4 Threat Model:

- What specific attack types is the system designed to detect?
- Are there known attack vectors that flow-level analysis inherently misses?

8.5 Parameter Sensitivity:

- How sensitive is performance to the contamination parameter?
- Guidance on parameter tuning for different network environments?

Grammatical Corrections:

- "Using flow-level data reduces" → "**The use of** flow-level data reduces" (more formal)
- "may miss payload-specific threats" → "may **fail to detect** payload-specific threats" (more precise)
- "The GUI's real-time feedback" → "The GUI's real-time feedback **mechanism**" (more complete)

9. CONCLUSION AND FUTURE WORK (Section 7)

The conclusion effectively summarizes the work and provides a reasonable roadmap for future research.

Strengths:

- Good summary of achievements
- Clear articulation of the system's value proposition
- Well-organized future work with specific directions
- Appropriate scope for extensions

Suggestions for Enhancement:

- Restate the key quantitative findings (with corrected accuracy figures)
- More explicitly state the main contributions to the field
- The future work section is quite extensive consider whether some items might actually be limitations of the current work that should be in the Discussion
- Could add a brief statement about the broader impact on cybersecurity practices

Grammatical Corrections:

- "This study has demonstrated the feasibility and effectiveness in developing" → "This study **demonstrates** the feasibility and effectiveness **of** developing" (simpler tense, correct preposition)
- "making it suitable for modern network environment" → "making it suitable for modern network **environments**" (plural)
- "where speed, adaptability, and interpretability are highly essential" → "where speed, adaptability, and interpretability are **essential**" (remove "highly" either something is essential or not)
- "The overall framework highlights that Python's environment, built around robust libraries" → "The framework **demonstrates** that Python's ecosystem, **with its** robust libraries" (clearer phrasing)
- "it can effectively support developing" → "**can effectively support the development of**" (more formal)
- "That makes the system" → "**This makes the system**" (more formal)
- "For future work, several extensions are envisioned to further increase the scalability, intelligence, and scope of operations of the system" → "For future work, several extensions are envisioned to **enhance** the scalability, intelligence, and **operational** scope of the system" (more concise)

10. REFERENCES

The reference section is inadequate for a research paper were not cited in your work, ensure you cite all your references.

Critical Issues:

- Only **three references** this is far too few for a research paper
- No foundational papers on Isolation Forest (Liu et al., 2008)
- Missing key IDS and network security papers
- No references for the datasets used
- Missing citations for scikit-learn, tkinter, and other tools

- The 2023 and 2024 papers in references should be cited in the text where relevant

Required Additions:

- Foundational machine learning papers (especially on Isolation Forest)
- Recent survey papers on ML for cybersecurity (2022-2024)
- Papers on flow-level traffic analysis
- Dataset papers (UNSW-NB15, CIC-IDS, NSL-KDD, or whichever was used)
- Comparative IDS studies
- Real-time system implementation papers
- Python scientific computing references

RATING SUMMARY

Criterion	Rating	Comments
Originality	**3 (Fair)**	The combination of Isolation Forest with GUI for flow-level IDS is practical but not highly novel. The core algorithm and approach are well-established. The contribution is more in implementation and accessibility than in methodological innovation.
Contribution to the Field	**3 (Fair)**	Provides a usable tool for practitioners but limited theoretical or empirical advancement. The work would be stronger with comprehensive comparative evaluation and validation on multiple datasets.
Technical Quality	**3 (Fair)**	The implementation appears sound, but the evaluation is insufficient. Missing: baseline comparisons, multiple datasets, statistical validation, ablation studies, and computational performance analysis. The low anomaly recall (46%) is concerning and inadequately addressed.
Clarity of Presentation	**2 (Good)**	Generally well-written and organized. The paper structure is logical, and most sections are accessible. However, several sections lack necessary technical depth, and there are inconsistencies in the reported metrics.
Depth of Research	**3 (Fair)**	The literature review is too limited (only 3 references), the experimental evaluation lacks comprehensiveness, and the discussion of limitations and comparative analysis is superficial. More thorough investigation is needed.

Overall Score: 2.8/4 (Fair to Good)

RECOMMENDATION

Decision: MAJOR REVISION REQUIRED

This manuscript presents a useful and practical implementation but requires substantial strengthening before it can be accepted for publication in a peer-reviewed journal. The work has merit, but the following major revisions are essential:

Critical Revisions (Must Address):

1. **Expand the literature review** significantly aim for more relevant references covering foundational ML work, recent IDS research, and comparative studies
2. **Resolve the inconsistency in accuracy metrics** clarify whether the system achieves 89%, 89.2%, or 95% accuracy and explain different metrics in different tables

3. **Add comprehensive comparative evaluation** compare against at least 2-3 other algorithms (Random Forest, SVM, One-Class SVM, autoencoder) on the same datasets
4. **Specify and describe the datasets** used name them, describe their characteristics, and cite them properly
5. **Address the low anomaly recall (46%)** this is a significant limitation that needs thorough discussion and potential improvement
6. **Add computational performance analysis** report processing time, memory usage, latency, and scalability metrics
7. **Include ROC curves and AUC score** these were mentioned as key metrics but never shown
8. **Expand the methodology section** provide much more detail on feature extraction, preprocessing, and the detection pipeline

Important Revisions (Should Address):

9. Expand the discussion section with critical analysis of limitations, failure cases, and parameter sensitivity
10. Add ablation studies or sensitivity analysis to understand component contributions
11. Improve the Related Work section with critical analysis and comparison of approaches
12. Include statistical significance testing for results
13. Add pseudocode or algorithmic descriptions for key components

Minor Revisions:

14. Correct all grammatical issues identified above
15. Ensure consistent terminology throughout
16. Add more specific details to the abstract
17. Improve figure quality and ensure all figures are properly referenced in text

---

Note: This review is intended to be constructive and supportive. The identified issues are addressable, and the core work shows promise. The requested revisions will significantly strengthen the manuscript's contribution and impact.